

METHOD, SYSTEM, SERVER AND DEVICE FOR MAKING A
COMMUNICATIONS NETWORK SECURE.

Ins A' >

As an increasing number of companies are connecting to networks and in particular to Internet, security on computer networks becomes an important issue at the dawn of the twenty-first century. Many
5 problems arise in companies and other organizations. These problems are usually referred to under the term of computer hacking; the people who are responsible for this are referred to as hackers.

09/720542 122200

10 This computer hacking has several facets. For example, it may be performed from outside or from the inside of 'the company', this term 'company' referring to a firm of an industrial or commercial nature, a government organization or any other association of interests. Further it may have different goals: alter,
15 suppress, peruse data (read, change or delete); or prevent the computer network from operating properly (notably by remotely impairing the operation of the essential computers).

Before continuing, hacking methods shall have to
20 be discussed, those that may be described as physical methods because they are based on physical characteristics of the computer systems.

The first and the most simple of these physical methods is what is called in computers, 'sniffing'.
25 This corresponds to physical spying of connection cables. The hacker may thereby capture all the information which transits within this network. The hacker may obtain vital information: confidential information of any nature, network user passwords. He
30 may also alter or delete these data.

002227 " 2450260

5 A second method of physical hacking requires very considerable means. It is based on intercepting electromagnetic waves emitted by a computer screen (or emitted by any component of the computer system). Another physical hacking method consists in perusing typed texts by simple observation while it is being typed on the keyboard or during its display on the screen. (Direct or indirect observation of the user).

10 These physical methods are undetectable for the computer system and are independent of this system.

Except for these physical methods, computer hacking may also be based on methods which will be termed as logical methods. These methods directly tackle the computer system's logic.

15 Generally they make use of the weak points of this logic. Most of these methods frequently use what is called a trap, i.e. a loophole in an operating system or in another software package. These traps are entry points in a computer system which pass over the normal security measures. This may be a concealed program inside the computer system or an electronic component which makes the protection system inefficient. Further, the trap is often enabled by an event or a "normal" action. The trap may also be a voluntary loophole in the security system. In this case, the traps are not always harmful: certain operating systems have user accounts with high privileges for facilitating the work of maintenance technicians.

20
25
30 In order to understand these logical methods, it should be brought to mind that every time a user makes a request in order to access a file or more generally a computer resource, the operating system decides whether

5

10

20

30

communicate with each other, they must first be authenticated one by the other, i.e., use a common encipherment key. Presently this authentication process is numerical and is based either on a code typed in by the user or on a code logically generated by both computers. In this second case, unfortunately, both computers have to exchange a sequence of information until they mutually authenticate each other. It follows that a third computer entering and hacking this system may locate the generated code by perusing over this exchange of information. By doing this, it may have access to the transmitted data and may even usurp the identity of these hacked machines.

Data encryption is also used for making information contained on a computer data medium incomprehensible. In this case, the enciphering keys are generated in the same way as for encipherment of transmissions.

All enciphering methods presently used are based on mathematical algorithms. There are two encipherment algorithm classes: symmetrical algorithms and asymmetrical algorithms.

The symmetrical algorithm only uses one single enciphering key which therefore serves both for encrypting and decrypting data at the same time. Conversely, the asymmetrical algorithm uses two keys: a public key and a private key. In this second enciphering method, each user has two keys: a private key and a public key. His public key is known to all the other users. With it, the message may be encrypted but not decrypted. His private key is only known to him exclusively, and is unknown to the other users. With it, the enciphered message may be decrypted.

09720542-122200

An asymmetrical system may be used for a key exchange protocol, i.e., a protocol enabling two users to agree on a symmetrical encipherment key to be used for the actual encipherment.

5 An example of such a protocol is detailed in US-4200770 et CA-1121480. As an example, and for a better understanding of the present document, this asymmetrical algorithm is described hereafter.

10 In the rest of the present document, the notation $g^a[N]$ represents g to the power of a , modulo N .

15 Let A et B be two users of the algorithm. Each user has a confidential private key, for example ' a ' for A et ' b ' for B . The numbers $g^a[N]$ and $g^b[N]$ are known to all. Numbers g et N are fixed and chosen once
20 and for all by A and B , in such a way that the multiplicative group for the successive powers of g modulo N has a large number of elements. Practically, N is chosen to be a very large prime number with for example about a hundred of decimal figures and such
25 that $(N-1)/2$ is prime, and that g is a primitive root modulo N , i.e. a generator for the multiplicative modulo N group.

30 When A wants to communicates with B in such a way as to be only understood by B , A takes the public key of B : g^b and raises it to the power of ' a ' (always modulo N) which gives $g^{(ba)}$ and thus provides the encipherment key for a symmetric algorithm. B is the only one able to understand the message by doing
35 $(g^a)^b = g^{(ab)} = g^{(ba)} [N]$.

40 This method works because there is no known algorithm for solving within a reasonable time, the ' x ' equation: $g^x = d [N]$ if N is very large.

Private keys ' a ' and ' b ' of A and B are usually

002227 24502460

generated by random number generators upon first communication between the two speakers. As these numbers are not always stored, they must now be regenerated regularly.

5 The encipherment algorithms presently used are
very efficient. However, user authentication is not
fully satisfying. In the case of direct authentication
between two encipherment devices (therefore without any
human intervention), a third encipherment device may
10 manage to impersonate one of the other two devices and
may thus access data on the other computer, as already
mentioned. If the authentication requires that a code
be typed in by the user on the keyboard of his
computer, this code may be intercepted by a hacker or
15 may be directly observed when it is typed in on the
keyboard.

There is a third known method against hacking. This method is related to the protection of internal networks. In order to prevent intruders from penetrating into an internal network, several companies have introduced on the market, locks (more commonly called "firewalls" by computer specialists). This is a logical barrier between the company's network and a network which has not been made secure (for example, Internet). A lock is a device placed on a specific computer which prevents unauthorized accesses to information resources of the internal network. In other words, a lock operates like a gateway by monitoring information flowing in both directions. It is able to prevent certain external users from accessing certain data or software resources of the internal network. Thus, security problems of the internal network with regards to the outside world, are normally confined in

one single point of the network: the lock.

002227" 24502260
This lock, if it is properly used (alas, this is the case very rarely), is logically impenetrable. So, one will have to resort to another approach: for instance, the hacker will prevent the computer hosting the lock from properly operating by saturating it with messages sent to it profusely which will force this computer to exceed its information processing capabilities. If this computer is no longer running, the hacker may then penetrate into the network which is no longer made secure by the lock.

Further, a lock is no protection against a possible hacker directly working within the network. Unfortunately, this case is not an exception and according to the FBI, more than 80% of the hackings would be due to a person having an internal access to the network.

In order to defeat computer hacking in addition to the aforementioned prevention techniques, an attempt may also be made to find out who the author of this hacking is. It is possible to make use of the computer traces left behind him: opening of files, connections with servers... indeed, most computer handling operations leave digital traces in the operating systems. Unfortunately, it is rather easy to conceal these traces: usurping somebody's identity by using his password, borrowing a workstation so as to have someone else accused, are standard hacker techniques and are very easily implemented. Indeed today, user authentication is performed through his digital identifier but not by recognizing the physical person. As a result, one can never be absolutely certain of the identity of the user of a computer.

5

10

15

25

- 30

[illegible]

still by his finger prints or a picture of his retina). This information is specific to each user and is sent to the authentication management server. This server then checks whether the relevant user is authorized to use the network component equipped with the device according to the invention which has just sent the authentication request. The server then sends back to the device according to the invention, its consent or it reports that the user is not authorized to use said network component.

This method provides distributed and dynamic security on a computer network. Indeed, security is supported by interconnected devices between each computer equipment which should be made secure and the communications network. The security of these devices is managed by a central server which receives information from all these devices. The server may now choose an overall security policy which will then be applied at each of the devices.

This security is configurable and it may develop over time according to new needs or modes of attack.

Indeed, a more flexible management of the network is achieved by having this list of security parameters sent by an authentication management server. The sent information may be very simply changed on the authentication server. User access authorization may thereby be changed easily.

Specifically, it should be noted that the security parameters depend on:

- the user,
- the network component which he desires to use,
- the security level which he has selected,
- the date and time,

communications protocol (for example TCP/IP, FTP, POP, etc.) has certain properties which are easy to check. If the packet does not have them, it is considered as invalid. This operation is usually performed by the
5 operating system or by a lock. The device according to the invention may therefore alleviate the task of the network component to which it is connected.

One should be aware that the computer hacker often uses badly formed packets sent in a great number onto
10 the machine to be hacked in order to increase the operational load of this machine with the purpose of interfering with its operation.

The security parameters enabling the messages related to said client/server applications to be
15 analyzed may also contain a list of communication ports. One should be aware that each software package which needs to communicate with the network, uses a certain communication port. For example, in order to read electronic mail, a well-defined port must be used,
20 another one has to be used for examining Internet sites.

Thus, an application may already be well characterized by a simple list of communication ports.

Hackers often use a Trojan horse, i.e. a program
25 placed on the target machine which will enable the hacker to perform certain tasks thereon. Now, a Trojan horse needs a communications port in order to receive orders from its designer. When a packet passes through the device, the device's processing means check whether
30 this packet is using an authorized port. Thus, a given user may be prevented from accessing to the Internet or a Trojan horse may be prevented from chatting with its designer.

09720542 122200

112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107

10

- 15

20

- 25

With this method, a system may be designed for partitioning the network components.

30

- the step for customizing the device with a private encipherment key provided by means of the authentication module,

- the step for storing, by means of the server, all the public encipherment keys associated with the private encipherment keys which customize the devices.

5 Advantageously, the security parameters further comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with, in an enciphered way,
- 10 - the public encipherment key of each piece of computer equipment which the user is also authorized to communicate with, in an enciphered way.

15 Advantageously, the method according to the invention further comprises the following steps:

- the step for enciphering by means of the device, communications by combining the private encipherment key of said device with the public encipherment key of the computer equipment which the user is authorized to communicate with, in an enciphered way.
- 20

In this operating mode, each device is customized by a private encipherment key allowing an encipherment key exchange protocol to be executed. This private key is associated with a public encipherment key registered in the list of pieces of computer equipment which the user is authorized to communicate with, in an enciphered way.

25 As a reminder, if the asymmetrical algorithm from US-4200770 is used, the private key is written as 'a' and the public key is written as $g^a [N]$.

30 The present invention provides a system for distributively and dynamically making a communications

002222T 24502260

applications,

- information enabling the devices to analyze the messages related to said client/server applications.

5 Advantageously, the processing means of the device comprise:

- means for analyzing the messages related to said client/server applications,
- means for filtering the messages related to said client/server applications,
- 10 - means for changing messages related to said client/server applications.

Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with.

15

Advantageously, said processing means of the device comprise:

- means for allowing messages to be transmitted between the piece of computer equipment to which the device is connected and the computer equipment which the user is authorized to communicate with,
- 20 - means for blocking messages between the piece of computer equipment to which said device is connected and computer equipment which the user is not authorized to communicate with.

25

Advantageously, the system according to the invention comprises:

- an authentication module associated with the device customized by means of a private encipherment key which customizes the device with which it is associated,
- 30 - a server storing all the public encipherment keys associated with private encipherment keys which

002221-24502450

customize the devices.

Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with, in an enciphered way,
- the public encipherment key of each piece of computer equipment which the user is authorized to communicate with, in an enciphered way.

Advantageously, the devices comprise:

- an encipherment module for enciphering communications by combining the private encipherment key of the device with the public encipherment key of the computer equipment which the user is authorized to communicate with, in an enciphered way.

The present invention provides a server for distributively and dynamically making a communications network secure, notably of the Internet type, characterized in that it comprises:

- processing means for processing information from a device and related to a user of a piece of computer equipment to which this device is connected,
- said processing means enable the user to be authenticated with the help of said information,
- management means for managing the authentications,
- transmission means for transmitting the security parameters to the devices of the network.

Advantageously, the security parameters comprise:

- a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server

00222T "24502260

applications.

Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with.

5 Advantageously, the server according to the invention comprises:

- storage means for storing all the public encipherment keys associated with the private encipherment keys which customize the devices.

10 Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with, in an enciphered way,
- the public encipherment key of each piece of computer equipment which the user is authorized to communicate with, in an enciphered way.

15 The present invention provides a device for making a communication network secure, interconnected between each piece of computer equipment which is to be made secure and said network and characterized in that it comprises:

- 20 - two input/output interfaces for intercepting communications between a piece of computer equipment to which it is connected and its communications network,
- 25 - an authentication module for obtaining information related to a user of the piece of computer equipment to which said device is connected and for defining the security level of said device,
- 30 - means for transmitting information related to the user and the security level of the device, to an authentication management server,
- storage means for storing security parameters from

002221 24502.60

the server,

- processing means for processing said security parameters from the server.

Advantageously, the security parameters comprise:

- 5 - a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server applications.

10 Advantageously, said processing means of the device comprise:

- means for analyzing the messages related to said client/server applications,
- means for filtering the messages related to said client/server applications,
- 15 - means for changing the messages to said client/server applications.

Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with.

20 Advantageously, said processing means of the device comprise:

- means for allowing messages to be transmitted between the piece of computer equipment to which the device is connected and computer equipment which the user is authorized to communicate with,
- 25 - means for blocking messages between the piece of computer equipment to which the device is connected and computer equipment which the user is unauthorized to communicate with.

30 Advantageously, the authentication module associated with said device provides:

- a private encipherment key which customizes said

0022221 24502760

device.

Advantageously, the security parameters further comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with, in an enciphered way,
- the public encipherment key of each piece of computer equipment which the user is authorized to communicate with, in an enciphered way.

Advantageously, the device according to the invention comprises:

- an encipherment module for enciphering communications by combining the private encipherment key of said device with the public encipherment key of the piece of computer equipment which the user is authorized to communicate with, in an enciphered way.

Thus, a computer equipment may communicate with another computer equipment in an enciphered way. The packet to be sent is enciphered by an encipherment module with the help of the encipherment key corresponding to the address of the other piece of computer equipment. The packet received from the network is deciphered by the private encipherment key of the device.

For a better understanding of the invention, several embodiments thereof will now be described, as purely illustrative and non-limiting examples.

In the drawing:

Fig. 1 shows a general diagram of a computer network made secure through the invention.

Fig. 2 shows a general diagram of a first embodiment of the device according to the invention.

00222T 24502760

InsAs 25

Fig. 3 shows a general diagram of a second embodiment of the device according to the invention.

Fig. 4 shows the second embodiment of the device according to the invention when it is implemented in a computer.

Fig. 5 shows the second embodiment of the device according to the invention when it is on the outside of a computer component as an external module.

Fig. 6 shows an embodiment of the encryption module 7.

Figs. 7 and 8 show an embodiment of the device according to the invention when it is miniaturized in a chip.

Fig. 1 shows a general diagram of a network made secure through the invention. This may be an internal network of a company, a public network like Internet or a mixed network, i.e. one or more internal or external networks connected with each other. This network is made up of 7 computer components noted as A, B, C, D, E, F, G which may be a computer, a computer server, a portable computer, a printer server, a printer... These computer components are equipped with the device according to the invention. The network has an authentication management server S. Two users of this network have be illustrated: a user U using component A of the network and a user U' who may use component B of the network.

Fig. 2 shows a general diagram of a first embodiment of the device according to the invention, made up of a microprocessor 1, connected through a data bus 2 to a memory 3, to two input/output interfaces 8 and 9, to a user authentication module 6 and to an encryption module 7.

00222T " 24502460
ns at

Fig. 3 shows a general diagram of a second embodiment of the device according to the invention, wherein a data reader 4 connected to a data bus 2 and a data medium 5 specific to each user have been added.

5 Fig. 4 shows the case when the device according to the invention is placed in a computer A connected to an Ethernet network 12, using the communications protocol: 'Transport verification protocol' commonly called
10 'Transport Control Protocol' or TCP within the 'Internet protocol' framework, commonly called the Internet protocol or IP which will be referred in what follows as the TCP/IP communications protocol.

The device according to the invention is then made up of an electronic card 10 which is placed in computer
15 A and which bears the microprocessor 1, the encryption module 7, both input/output interfaces 8 and 9 (the latter optionally included in 1) and memory 3. The microprocessor 1 is connected through a series connection to a chip card reader with a keyboard. This
20 reader comprises both the data reader 4 and the authentication module 6 which will be noted as 4 + 6.

Each user has a chip card as data medium 5 containing his identification number, the user private key 'u' for encrypting communications with the
25 authentication management server S described in Fig. 1 as well as the IP (Internet Protocol) address and the public key of said server S. Each chip card also contains one or more personal encryption keys and a list of authorized communications ports. The encryption
30 module 7 is based on a block algorithm. The input/output interface 8 is an interface providing connection to a PCI bus, the other interface 9 providing connection to the Ethernet network 12.

00222T"24502260

The electronic card of computer A sends the
 identification number of user U, in an encrypted way,
 to the authentication management server S, by using the
 encryption key ($g^{as} [N]$) which it solely possesses
 5 with the authentication management server S ('s'
 indicates the private encryption key of the server).
 Indeed, the authentication management server S has
 access to all public keys, therefore it is aware of g^a
 $[N]$, and may therefore calculate $g^{as} [N]$. On its side,
 10 A is aware of its private key 'a' and of the public key
 $g^s [N]$ of server S and may therefore calculate g^{as}
 $[N]$ on its side. The message may now be encrypted by A
 and decrypted by server S. Server S then consults its
 table in order to determine the list of TCP/IP
 15 addresses which the user U may communicate with, and
 for each address, the public encryption key associated
 with this address. Furthermore, it identifies the IP
 address of computer A with user U.

The authentication management server then sends to
 20 the device according to the invention which equips
 computer A, the list of authorized addresses for user U
 as well as their public keys and the list of authorized
 communications ports for this user. This sending always
 occurs in an encrypted way but this time, by using key
 25 $g^{su} [N]$ (where 'u' represents the user's private key
 for encrypting communications with the authentication
 management server S). The microprocessor 1 of the
 electronic card 10 placed in computer A then stores
 this list.

30 In order not to impair the network's operation,
 the microprocessor 1 calculates the encryption keys
 $g^{ab} [N]$ (where 'b' is the private key of any other
 network component B) when it has nothing else to do.

002227 "24502460

The calculated keys are then stored by microprocessor 1. These keys will be deleted as soon as the user removes his chip card 5 from reader 4.

When an information packet arrives (from the
5 network or from the central processing unit (CPU) of
the computer), processor 1 must unwrap the TCP/IP
protocol in order to find: the communications port used
by the packet, the address of the addressee (if the
packet comes from the CPU) or of the sender (if the
10 packet comes from the network). This address will be
called 'packet address' in the rest of the document.
This unwrapping of the packet allows certain invalid
packets to be detected which no longer observe all the
criteria of the TCP/IP communications protocol. Details
15 on the TCP/IP unwrapping are explained in the book by
Mr. Guy Pujolle 'Les réseaux' on pages 539-579.

When computer A communicates with another
component of the network, for example computer B, the
microprocessor 1 checks whether the port used by the
20 packet belongs to the list of authorized ports. Then
the microprocessor 1 examines the packet's address: if
it belongs to the authorized addresses, the packet is
processed, otherwise the packet is ignored. In the
first case, the microprocessor searches whether the
25 encryption key ($g^{ab} [N]$) required for communications
between A and B, has already been calculated. If this
is not the case, the microprocessor calculates the
missing key. Once the encryption key ($g^{ab} [N]$) is
known, the packet is encrypted if it comes from the CPU
30 or decoded if it comes from the network, then the
processor regenerates the TCP/IP wrapping. Thus, the
communications are well-customized between two pairs of
network components equipped with the device according

002227 "24502260

to the invention.

Under the assumption that the address of computer B is in the list of network components which user U of computer A is authorized to communicate with, the
5 microprocessor 1 of the electronic card 10 placed in computer A may calculate the encryption key ($g^{ab} [N]$) which will be used by the DES chip for communicating in an encrypted way with the other computer B. A distinction must now be made between several working
10 cases of computer B:

a) There is a user U' on computer B. This user U' also has certain public keys including the one of A. Communications then take place without any problems.

b) There is a user U' on computer B. However, this
15 user U' does not have access to computer A. User U of computer A therefore cannot communicate with computer B as he would risk affecting the system's security.

c) There is no user on computer B. The device according to the invention connected to computer B asks
20 the authentication management server S whether user U is authorized to have access to computer B as nobody is keeping a watch on him. If the device according to the invention associated with computer B obtains this permission, the public key of the device according to
25 the invention connected to computer A, will be sent back to it by the authentication management server S, exclusively.

d) No user was using computer B but user U had obtained permission from the authentication management
30 server to communicate with B. The arrival of a user U' on computer B leads to alternatives a) or b).

e) Computer B was being used by user U' who then stops using the invention by removing his chip card.

002222T "24502260

required security level.

In another embodiment of the invention illustrated in Fig. 5, where each device according to the invention is not placed in a computer, but placed as an independent module on the network, it may be contemplated that the device according to the invention is then not customized by a private encryption key contained in memory 3 but by a private encryption key contained on the data medium 5 specific to each user; this key is read as soon as the user is authenticated by the authentication module. In this embodiment illustrated in Fig. 5, the device according to the invention is made up of an electronic card 13 bearing the microprocessor 1 connected through several buses 2 to: a memory 3, an encryption module 7, both input/output interfaces 8 and 9 which, in this embodiment, are network interfaces providing for example the Ethernet wrapping in the case of an Ethernet network. The data reader 4 may further be coupled with an authentication module 6 as a chip card reader which may be placed on the electronic card 13 or which may be external to the above described module according to another embodiment.

The components used in this embodiment may be those used in the first embodiment.

Operation of the module is identical to the operation of the device according to the invention as described in the first embodiment except as regards the private encryption key. This key must be read as soon as the user is identified with the help of the identification module 6 so that the encryption keys $((g^{ab} [N]))$ may be calculated.

It should be noted that the chip card reader may

00222T" 24502260

be replaced with a finger print reader or with the reader for the retina of the user. The address of the authentication management server S is then contained in memory 3 as well as its public encryption key. When the user is authenticated with the help of the authentication module 6, this module 6 then has the digital information on the user, which it sends to the microprocessor 1. The latter then uses part of this information (for example the first 128 bits) in order to form the private key 'u' of the user for encrypting communications with the authentication management server S.

Everything then takes place as in the case of the chip card reader except for the fact that the user must report when he ceases using the device according to the invention, for example by pressing on a button.

Fig. 6 illustrates in more details an embodiment of the encryption module 7, part of the device according to the invention. Now, 12 DES chips arranged in columns of four are inserted; these chips are referenced by notation $P_{i,j}$ where i is the index of the column and j that of the line. Two mixers M1 and M2 are also added.

This encryption module operates with any block encoding algorithm, whereby the latter may be performed by a software package or by a specific hardware device. In order to simplify the test and to emphasize the analogy with algorithms of the DES triple type detailed later on, an example based on the use of a DES chip will be discussed.

The DES algorithm operates with a 56 bit key on messages cut up into 64 bit packets. Triple DES is an encoding algorithm based on the use of three successive

002221-2450260

DES algorithms and which may be implemented by using three DES chips. A packet to be encrypted crosses the first chip and is encrypted with a first encryption key, it then crosses the second DES chip and is
 5 encrypted with a second key, but by using here the DES inverse algorithm. It then crosses the third DES chip where it is again encrypted with the first key.

Mixers are available commercially which allow a message to be mixed: 'n' input bits are mixed by the
 10 mixer which provides 'n' output bits but in a different order. This order may be redefined by a number, every time. This mixing function may be reduced to a table look-up and it may be performed by software on the microprocessor 1 contained in the invention or by a
 15 programmable component.

By coupling several DES chips with such a component, a DES may be designed which works on much larger packets. For example, let 12 DES chips be placed in rows by 4. The first 4 are placed in parallel and
 20 process a message of 4 times 64 bits (the chips simultaneously operate with encryption keys K1,1, K1,2, K1,3, K1,4, for chips P1,1, P1,2, P1,3 and P1,4, respectively). Subsequently, the message crosses a mixer M1 (controlled by key X). The message then
 25 crosses a new row of 4 DES chips P2,1, P2,2, P2,3, P2,4 in parallel (controlled by keys K2,1, K2,2, K2,3, K2,4). In this second row of chips, the used algorithm is the inverse of the one used in the first and second rows (as in triple DES). Then the message crosses through
 30 another mixer (controlled by key X^{-1} in order to perform inverse mixing). Finally, a last row of 4 DES chips, P3,1, P3,2, P3,3, P3,4 (controlled by keys K3,1, K3,2, K3,3, K3,4) processes the message.

0022221"24502/50

This set-up may be completed in three phases with a single DES chip and a single mixer, provided that the intermediate results are stored. For this, in a first phase, the 4 times 64 bit message to be processed is cut up into four 64 bit packets. The first packet crosses the chip controlled by key $K_{1,1}$ and the result is stored. Then the second packet crosses the chip this time controlled by key $K_{1,2}$, the result is stored. In the same way, the third packet is encrypted by key $K_{1,3}$, then stored. Finally, the fourth packet is encrypted by key $K_{1,4}$ and stored.

Each of these four packets encrypted with the help of (64 bit) keys K1,1, K2,2, K1,3 and K1,4 enters the mixer and is then stored, and cut up into four new small 16 bit packets. The first 16 bit sub-packets issued from the encrypted and mixed 64 bit packets are combined, forming a new 64 bit packet which in turn is mixed.

This is repeated a third time as described in the
20 above paragraphs after replacing encryption keys K2,1,
K2,2, K2,3, and K2,4 with keys K3,1, K3,2, K3,3 and
K3,4. Of course, in this third pass, information does
not necessarily pass through a mixer. A very high
security version may be designed with 12 different keys
25 for the DES and with two other keys for the mixers. The
entire key may have for example 1024 bits in order to
maintain a power of 2 (56 times 12, i.e. 672 bits for
the DES, the keys for the mixers may be much longer).

The symmetry of triple DES may be maintained by
30 using identical keys in the first and third phases,
i.e. $K_{3,1} = K_{1,1}$, $K_{3,2} = K_{1,2}$, $K_{3,3} = K_{1,3}$ and
 $K_{3,4} = K_{1,4}$ (the entire key will then have a size of
512 bits) or by producing a simpler version for the

which are found for example on PCI/Ethernet network cards.

Chip 100 is described in Fig. 7. This type of chip is usually called a 'system on a chip' by computer
5 specialists.

The chip is then made up of a processor core 1 (for example a ARM 7 from the ARM company) connected through a 32 bit bus 141 to:

- a memory controller 131 which controls external
10 memory 3
- a bridge 140, enabling several buses to be connected with one another
- a double access memory block 103 internal to the chip.

15 Bus 143 is connected to memory 103. Both buses may thus read and write into memory 103. Bus 143 is connected with 3 input/output interfaces 8, 8bis and 9. Interfaces 8 and 8bis are network interfaces (for example Ethernet) supporting all the link and physical
20 layers of the ISO standard (encapsulation, transport...). Upon implementing chip 100 on card 13, the input/output interfaces to be used are selected (for example network/network, for an external embodiment or network/bus for an embodiment internal to
25 the computer).

Thus, this embodiment allows a unique chip 100 to be produced with which an internal or external device may subsequently be built very simply.

30 Bus 142 is connected to a serial interface (RS232) enabling the chip card reader 4 to be controlled. It is possible to add other RS232 interfaces on this bus, for example, for connecting chip 100 to a V-modem or simply for controlling the diodes placed on card 13.

The operation of the module is identical to the operation of the invention as described in the first or second preferred embodiment: everything depends on the private encryption key which may be placed either in
5 chip 100 (as in the first embodiment) or provided by the user (as in the second embodiment).

It is well understood that the different embodiments described above are purely illustrative and non-limiting and that many alterations may be made to
10 them without however departing from the scope of the invention.

It should be noted that the chip card reader may be replaced with a finger print reader or with a reader for the retina of the user.

0022221 24502/60